UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

- against -

FRANK DiTOMASSO,

Defendant.

OPINION AND ORDER

14-cr-160 (SAS)

SHIRA A. SCHEINDLIN, U.S.D.J.:

I. INTRODUCTION

Frank DiTomasso has been charged with producing and transporting child pornography. Much of the Government's case against DiTomasso depends on evidence procured through searches of his computer — searches carried out pursuant to a warrant that was issued, in part, on the basis of evidence obtained by America Online ("AOL") and Omegle.com ("Omegle") when they monitored DiTomasso's emails and chats. DiTomasso believes that by reviewing the content of online correspondence, AOL and Omegle violated his Fourth Amendment rights, because (1) he had a reasonable expectation of privacy in the content of his emails and chats, and (2) AOL and Omegle were operating as agents of law enforcement. On this theory, DiTomasso moved to suppress chats and emails, as well as any other "information and tangible and intangible evidence obtained

through subsequent searches by [law enforcement]" as fruit of the poisonous tree.[1]

On October 28, 2014, I ruled that DiTomasso had a reasonable expectation of privacy in the content of both his emails and his chats.[2] I also ruled, however, that DiTomasso consented to a search by AOL in a law enforcement capacity when he agreed to its terms of use — defeating his suppression motion as to AOL.[3] But the motion is still live as to Omegle, and now the Court must resolve the question explicitly reserved in the October 28, 2014 Opinion. Namely, was Omegle operating as an agent of law enforcement when it reviewed screen shots of DiTomasso's chats and — believing that they contained evidence of child pornography — dispatched three reports to the National Center for Missing and Exploited Children ("NCMEC Reports")?

For the reasons set forth below, I conclude that the answer is no. Omegle's monitoring constituted a purely "private search," beyond the reach of the Fourth Amendment. Accordingly, DiTomasso's motion to suppress is DENIED.

II. BACKGROUND

---

[1] Memorandum of Law in Support of Motion to Suppress ("Def. Mem."), at 1.

[2] *See United States v. DiTomasso*, No. 14 Cr. 160, 2014 WL 5462467 (S.D.N.Y. Oct. 28, 2014).

[3] *See id.* at *9.

Omegle monitors its chats "for inappropriate content . . . by capturing snapshots from chats that are conducted on Omegle,"[4] which are then "analyze[d]" by an automated program "for content that is likely to be inappropriate, including, but not limited to, child pornography."[5] When the automated program flags inappropriate content, the chats are "passed on to two human reviewers,"[6] and if a reviewer finds evidence of child pornography, she issues a NCMEC Report.[7]

The issuing of NCMEC Reports is obligatory under section 2258A of the PROTECT Our Children Act,[8] which requires any private entity that "obtains actual knowledge" of child pornography trafficking to notify NCMEC.[9] The statute also provides a safe harbor for compliance. Under section 2258B, any entity that issues a NCMEC Report pursuant to its obligations under section 2258A is immunized from all liability, civil or criminal, that might otherwise have resulted

---

4 Declaration of Lief K-Brooks, Founder of Omegle.com ("K-Brooks Decl."), Exhibit C to Government's Memorandum in Opposition to the Motion to Suppress ("Opp. Mem."), ¶ 3.

5 *Id.* ¶ 4.

6 *Id.*

7 *See id.* ¶ 5.

8 *See* 18 U.S.C. § 2258A.

9 *Id.* § 2258A(a)(1).

from the nonconsensual disclosure of a user's electronic information.[10] There is, however, no statutory obligation to *look for* child pornography trafficking. Rather, the obligations of section 2258A are triggered only when an internet service provider ("ISP") like Omegle obtains "actual knowledge" of such trafficking. Section 2258A(f) makes clear that

> [n]othing in [section 2258A] shall be construed to require an electronic communication service provider or a remote computing service provider to monitor any user, subscriber, or customer of that provider; monitor the content of any communication of any person; or affirmatively seek facts or circumstances [related to the trafficking of child pornography].[11]

According to Omegle's founder, Lief K-Brooks, the company began "monitoring chats in November 2012, as an effort to improve the user experience by removing inappropriate content from the site."[12] The decision stemmed from K-Brooks' perception that "[a]t [the] time, websites offering anonymous chat services were receiving negative media attention for the amount of inappropriate

---

[10] *See id.* § 2258B(a) ("a civil claim or criminal charge against an electronic communication service provider . . . arising from the performance of the reporting or preservation responsibilities of such electronic communication service provider . . . under [a statute setting out mandatory reporting requirements for child pornography] may not be brought in any Federal or State court.").

[11] *Id.* § 2258A(f).

[12] K-Brooks Decl. ¶ 6.

content on their sites."[13] Wary of receiving such attention, K-Brooks "decided to implement [a] monitoring program."[14] As K-Brooks put it during the suppression hearing, he "wanted [his] site to be the best it could be for users," and he thought that "having inappropriate content on the site" was interfering with that goal — an impression gleaned from "feedback from users," as well as "media reports" and conversations with "friends [who] weren't as keen to use [the] site because of the amount of inappropriate content that it had."[15]

K-Brooks also clarified, however, that he knew Omegle was under no *obligation* to monitor its users' chats. To the best of his understanding, "if [Omegle] has actual knowledge of apparent child pornography, [it has] a duty to report it to the government, but no duty to monitor."[16] K-Brooks also testified that he made the decision to implement the monitoring program on his own[17] — possibly after conversations with "friends or family,"[18] but certainly without any

---

13 *Id.*

14 *Id.*

15 12/10/14 Transcript of Suppression Hearing ("12/10/14 Tr."), at 10.

16 *Id.* at 11.

17 *See id.* at 10-14.

18 *Id.* at 10.

input from law enforcement.[19]

In February 2013, Omegle developed an "unmonitored" version of its chat service.[20] This new feature allows users to opt-out of monitoring.[21] When asked why he decided to create an "unmonitored" version of Omegle, K-Brooks testified that it was, in effect, a concession to reality. Although ideally he would have preferred to excise all inappropriate content from the site, that goal seemed unrealistic — so he struck a compromise. In K-Brooks' words:

> I felt that, basically, people can evade a ban [of inappropriate material], no matter what you do, no matter how hard you try to keep them from getting around a ban, they can always find different technical means, whether that's clearing their cookies, changing their IP address, using a proxy, etc. So I felt it was better if those people who might be really intent to use the site but who I didn't want to be interacting with all the users, I felt it was better to give them an alternative path of least resistan[ce].[22]

When DiTomasso's counsel pressed him on this point at the suppression hearing, K-Brooks reaffirmed that he was opting for a lesser-of-two-evils approach. When

---

19 On this front, K-Brooks distinguished in his testimony between the question of *whether* to monitor users' chats, and the subsequent question of *how* to do so. As to the latter, K-Brooks acknowledged that he received input from various sources, including NCMEC and — possibly — law enforcement officials. *See id.* at 11-13.

20 *Id.* at 14.

21 *See* Opp. Mem. at 6 (explaining how the unmonitored section works).

22 12/10/14 Tr. at 14.

asked why he did not "just ban people on the monitored site and not create an unmonitored site for people doing what you fairly well knew was going to be inappropriate conduct,"[23] K-Brooks testified that "I mean, there's really no way to ban someone from a website and be completely sure that they [sic] can never come back again because the technology just isn't there yet . . . and if you just ban someone, then they might come back the next day."[24]

III. APPLICABLE LAW

The Fourth Amendment regulates state actors. Therefore, private parties are only bound by its requirements insofar as they operate as *de facto* state actors. As the Supreme Court explained in *United States v. Jacobsen*,[25] the Fourth Amendment is "wholly inapplicable to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any government official."[26]

One way for a private party to "act[] as an agent of the Government"

---

23 *Id.* at 25.

24 *Id.*

25 466 U.S. 109 (1984).

26 *Id.* at 113. *Accord Coolidge v. New Hampshire*, 403 U.S. 443, 487-89 (1971) (holding that it was a private search — outside the bounds of the Fourth Amendment — when a woman retrieved evidence against her husband from her home, and then gave it to the police).

is through legal compulsion. If a private party *must* perform a search — if she can face liability for not doing so — the search "is controlled by the Fourth Amendment."[27] But legal compulsion is not necessary for an otherwise-private search to be subject to the Fourth Amendment's requirements. A search carried out voluntarily by a private actor will still be subject to the Fourth Amendment's strictures if the government "demonstrate[s] a strong [] preference for [the search]."[28] For example, the Supreme Court has applied Fourth Amendment scrutiny to drug testing carried out by private railway companies, due to the existence of federal regulations that (1) precluded any collective bargaining agreement that forbade drug testing, (2) imposed specific penalties on employees who failed to submit to such testing, and (3) authorized the government to obtain test results.[29] Considering these facts and circumstances holistically, the Court concluded that the government had effectively "removed all legal barriers to the

---

[27] *Skinner v. Railway Labor Executives' Ass'n*, 489 U.S. 602, 614 (1989) (holding that it constituted a "search" when a private railroad company performed urine tests on its employees pursuant to a federal statute).

[28] *United States v. Stevenson*, 727 F.3d 826, 829 (8th Cir. 2013). *Accord Cassidy v. Chertoff*, 471 F.3d 67, 74 (2d Cir. 2006) ("Although a wholly private search falls outside the scope of the Fourth Amendment, a search conducted by private individuals at the instigation of a government officer or authority constitutes a governmental search for purposes of the Fourth Amendment.") (internal citations omitted).

[29] *See Skinner*, 489 U.S. at 615.

testing . . . [making] plain not only its strong preference for testing, but also its desire to share the fruits of such intrusions. . . . These are clear indices of the Government's encouragement, endorsement, and participation, and suffice to implicate the Fourth Amendment."[30]

Another way for a private party to "act[] as an agent of the Government" is to perform searches with an intent to assist law enforcement.[31] The law in this area is unsettled, and has not been addressed in the Second Circuit. But the Sixth Circuit has concluded, for example, that a private actor's reason for performing a search must be "entirely independent of the government's intent to collect evidence for use in a criminal prosecution" to escape Fourth Amendment

---

[30] *Id.* at 615-16. *Accord United States v. Knoll*, 16 F.3d 1313, 1320 (2d Cir. 1994) (explaining that "[t]he government may become a party to [an otherwise-private] search through nothing more than tacit approval"); *United States v. Wolfson*, 160 Fed. App'x 95, 98 (2d Cir. 2013) (explaining that "the government's knowledge or encouragement" of a search are factors to be considered in assessing whether the search is truly private).

[31] The notion that the purpose of a search bears on its constitutional status is already familiar in the "special needs" cases. In that setting, the question is whether a search was carried out primarily for the purpose of law enforcement, or primarily to advance some other end. *See Ferguson v. City of Charleston*, 532 U.S. 67, 74 (2001) (explaining that "our [] cases recogniz[e] that 'special needs' may, in certain exceptional circumstances, justify a search policy designed to serve non-law enforcement ends").

scrutiny.[32] Similarly, the Ninth Circuit has held that an otherwise-private search must comply with the Fourth Amendment if "its purpose [is] to elicit a benefit for the government in either its investigative or administrative capacities."[33]

IV. DISCUSSION

DiTomasso proposes two theories why Omegle was acting as an agent of law enforcement when it reviewed his chats. *First*, he argues that Omegle's monitoring program was implemented, in the first instance, with the goal of assisting law enforcement. *Second*, DiTomasso argues that regardless of *why* Omegle decided to begin monitoring chats, it was conscripted into a law enforcement role by the combination of (1) the reporting requirements set forth in

---

[32] *United States v. Bowers*, 594 F.3d 522, 526 (6th Cir. 2010) (internal citations omitted).

[33] *United States v. Attson*, 900 F.2d 1427, 1431 (9th Cir. 1990). This language is difficult to reconcile with the line of Supreme Court authority recognizing that permitting private persons to relay incriminating evidence to law enforcement serves "society's interest" in "bringing criminal activity to light." *Georgia v. Randolph*, 547 U.S. 103, 116-17 (2006). *Accord Coolidge*, 403 U.S. at 488 (holding that a woman's decision to give incriminating evidence about her husband to the police triggered no Fourth Amendment scrutiny despite being motivated by a law enforcement purpose). Nevertheless, because the Supreme Court has not definitively held that law enforcement purpose plays *no* role in the Fourth Amendment analysis, I adopt the standard articulated by numerous circuit courts, and endorsed by both parties to this litigation — that law enforcement purpose is one factor to consider when analyzing whether a search is purely private. *See* Opp. Mem. at 16 (explaining that "the private party's intent in executing the search" has been deemed relevant to the Fourth Amendment analysis by the First, Sixth, Ninth, and Tenth Circuits).

section 2258A, and (2) the guarantee of immunity in section 2258B.

A. Omegle's Monitoring Was for Business Purposes

There is no direct evidence to support the proposition that Omegle intended its monitoring program to assist law enforcement. In fact, at the suppression hearing, K-Brooks testified to exactly the opposite effect. He represented that Omegle began monitoring chats in an effort to staunch the "inappropriate content" flowing through its site. And when K-Brooks became concerned that monitoring, alone, was insufficient to meet this goal, he also set up an unmonitored section of Omegle, designed to quarantine "inappropriate content" to a specific, and self-selecting, population of users. Both of these decisions track the concerns — in essence, concerns about user experience — that K-Brooks articulated at the suppression hearing.

According to DiTomasso, K-Brooks' explanations are "not credible."[34] But DiTomasso marshals little evidence to support this view — and much of the evidence he does offer cuts the other way. For example, DiTomasso calls attention to the fact that in 2012, "Omegle received significant media attention when it was discovered that two individuals used Omegle to meet

---

[34] Supplemental Memorandum of Law in Support of Motion to Suppress Evidence (Dkt. No. 27), at 3.

underage victims."[35] But this merely underscores the need for monitoring and/or quarantining — which, if anything, makes K-Brooks' testimony *more* credible, not less. Similarly, DiTomasso argues that after considering the record holistically, the most likely explanation for K-Brooks' decision to develop an "unmonitored" section of Omegle is that he wished to "make[] additional ad revenue," *not* — as K-Brooks testified — that he wanted to "remov[e] inappropriate content" from the site. Even if this is true, however, it merely points to *another business rationale* for Omegle's monitoring practices. The Fourth Amendment is indifferent to whether K-Brooks wanted to purge his site of inappropriate content or, instead, to reap a monetary gain from its presence. The question is whether he *also* intended to catch criminals. And the answer, on this record, is no.

The picture that DiTomasso conjures — of ISPs like Omegle using their monitoring programs to play cyber-vigilante — is certainly plausible. Child pornography is despicable. In the abstract, it makes sense that many companies would like to discover it and report it. But there is no evidence that Omegle sought to aid law enforcement when it monitored users' chats for evidence of child pornography. Therefore, DiTomasso's first argument is unavailing.

B. Sections 2258A and 2258B Did Not Convert Omegle Into a Government Agent

---

35 *Id.* at 4.

Next, DiTomasso argues that regardless of what motivated Omegle to begin monitoring its users' chats, sections 2258A and 2258B effectively transformed Omegle — and similarly-situated ISPs — into agents of law enforcement. This argument has two prongs. *First*, it could be that *all* entities bound by the requirements of section 2258A, and immunized from suit by section 2258B, operate as agents of law enforcement, regardless of how much (or how little) the statutory scheme actually influenced an entity's decision to monitor. *Second*, it could be that this statutory scheme has the *practical effect* of encouraging monitoring — notwithstanding that neither section 2258A nor section 2258B bears on monitoring directly.

DiTomasso's claim fails on both prongs. An otherwise-private search only converts into a law enforcement search if the *search itself* is obligatory. A subsequent reporting obligation, which only goes into effect *if* a search is performed, is insufficient. As the Eighth Circuit has explained, both section 2258A and section 2258B "[are] silent regarding whether or how [an ISP] should scan its users' [activity]."[36] Indeed, "[t]he only subsection that bears on scanning" — section 2258A(f) — "makes clear that an [ISP] is *not* required to monitor any

---

[36] *Stevenson*, 727 F.3d at 830. *Accord United States v. Cameron*, 699 F.3d 621, 637-38 (1st Cir. 2012); *United States v. Richardson*, 607 F.3d 357, 366-67 (4th Cir. 2010). The Second Circuit has not addressed the issue.

user or communication, and need not affirmatively seek facts or circumstances demonstrating a violation that would trigger the reporting obligation of section 2258A(a)."[37] In light of this, I would be hard-pressed to conclude that sections 2258A and 2258B require private actors to perform law enforcement searches. Indeed, as the Government points out, an entity faced with reporting obligations under 2258A may well be "incentivize[d] [] *not* to monitor for child pornography, on the theory that they cannot be punished for failing to report what they do not know about."[38]

Turning to the second prong of the argument[39] — that although

---

[37] *Stevenson*, 727 F.3d at 830 (emphasis added). *See also* 18 U.S.C. § 2258A(f)(1)-(3) ("Nothing in this section shall be construed to require an electronic communication service provider or a remote computing service provider to monitor any user, subscriber, or customer of that provider; [or] monitor the content of any communication of any person . . . .").

[38] Opp. Mem. at 17 (emphasis added). *Accord Richardson*, 607 F.3d at 367 ("[I]f substantial fines are imposed for the failure to report known facts suggesting a violation of federal child pornography laws, ISPs and others subject to such penalties might just as well take steps to avoid discovering reportable information.").

[39] It bears noting that the courts of appeals that have considered whether the reporting requirement of section 2258A in effect requires ISPs to perform searches have addressed only the first prong. They have held that section 2258A generates no legal compulsion to search — and the analysis has ended there. *See Stevenson*, 727 F.3d at 830; *Cameron*, 699 F.3d at 637-38; *Richardson*, 607 F.3d at 366-67. As a result, no circuit court has addressed the distinct question of whether section 2258A has the *practical effect* of encouraging monitoring, notwithstanding the absence of a legal compulsion. The Supreme Court has made clear that in this

section 2258A is "silent as to . . . monitor[ing]," the reality is that ISPs feel pressure to monitor — the deficiency is factual, not legal. In his testimony at the suppression hearing, K-Brooks made clear that he appreciates the difference between an obligation to monitor and an obligation to report, and that he "understood" section 2258A — correctly — as imposing "no duty to monitor."[40] In the absence of countervailing evidence, I must accept this testimony at face value. According to its founder and CEO, Omegle felt no obligation to monitor its users' chats. It did so of its own accord. Thus, the decision raises no Fourth Amendment concern.

V. CONCLUSION

For the reasons set forth above, DiTomasso's motion to suppress is DENIED. The Clerk of the Court is directed to close this motion [Dkt. No. 16].

---

area, the proper inquiry is fact-bound — whether, in a functional sense, the government has "encourage[d]" or "endorse[d]" private investigative activity. *Skinner*, 489 U.S. at 615-16. It is possible to imagine circumstances under which the statutory scheme set forth in section 2258A, while not *requiring* searches, would nevertheless operate to encourage or endorse them in practice — for example, if ISPs received favorable treatment from law enforcement once they began reporting evidence of child pornography trafficking. However, no such circumstances are present in this case.

[40] 12/10/14 Tr. at 11.

SO ORDERED:

Shira A. Scheindlin
U.S.D.J.

Dated: New York, New York
January 26, 2015

- Appearances -

For Defendant Frank DiTomasso:

Lee Ginsberg, Esq.
Nadjia Limani, Esq.
Freeman, Nooter & Ginsberg
75 Maiden Lane, Suite 503
New York, NY 10038
(212) 608-0808

For the Government:

Margaret Graham
Assistant U.S. Attorney
Southern District of New York
One Saint Andrew's Plaza
New York, NY 10007
(212) 637-2923